UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/028,650	12/20/2001	Anton C. Rothwell	NAIIP056/01.187.01	2721

28875 7590 03/25/2008

Zilka-Kotab, PC
P.O. BOX 721120
SAN JOSE, CA 95172-1120

EXAMINER	
CHEA, PHILIP J	
ART UNIT	PAPER NUMBER
2153	

MAIL DATE	DELIVERY MODE
03/25/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/028,650	ROTHWELL ET AL.	
	Examiner	Art Unit	
	PHILIP J. CHEA	2153	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 January 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3-7,9,12-14,16-20,22,25-31 and 33-43* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3-7,9,12-14,16-20,22,25-31 and 33-43* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This Office Action is in response to an Amendment filed January 16, 2008. Claims 1,3-7,9,12-14,16-20,22,25-31,33-43 are currently pending, of which claims 42-43 are new. Any rejection not set forth below has been overcome by the current Amendment.

Claim Objections

1. Claims 1,3-7,9,12-14,16-20,22,25-31,33-43 are objected to because of the following informalities: the "capable to" language raises a question as to whether the intended steps are positively recited or if they are intended for future use. Appropriate correction is required.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1,3,6-7,12-14,16-20,25-31,34,38-40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Krishnan et al. (US 6,075,863), and further in view of Chi (6,006,329).

As per claim 1, Krishnan discloses a network adapter system, comprising:

a processor positioned on a network adapter coupled between an end-point computer and a network (see column 2, lines 33-39, where network adapter is considered the software-controlled modem), the network adapter capable of being installed on the end-point computer (see column 2, lines 44-50);

wherein the processor is adapted for virus scanning and content scanning of network traffic transmitted between the end-point computer and the network, the content scanning including scanning for unwanted content other than viruses (see column 5, lines 16-28, where processor executes applets to scan incoming data such as hazardous programs and viruses and content is considered "junk e-mail");

wherein the processor is capable of being user-configured (see Krishnan column 5, lines 33-35 and lines 55-57, where a user can buy an applet that is used to control modem (i.e. the modem processor));

wherein the processor is capable of determining whether received packets are of interest (see Krishnan column 5, lines 16-23, where packets of interest are considered viruses, etc.), passing received packets that are not of interest to the end-point computer (see Krishnan column 5, lines 16-23, i.e. if not a virus than packets is not discarded), and scanning received packets that are of interest (see Krishnan column 5, lines 16-23, i.e. scanning packets for viruses).

Although the system disclosed by Krishnan shows substantial features of the claimed invention (discussed above), it fails to disclose that the virus scanning utilizes virus signature files and that the virus signature files are stored on non-volatile solid state memory on the network adapter.

Nonetheless, these features are well known in the art and would have been an obvious modification of the system disclosed by Krishnan, as evidenced by Chi.

In an analogous art, Chi discloses scanning data streams for viruses (see Abstract) using virus signature files to detect known viruses (see column 3, lines 47-65).

Given the teaching of Chi, a person having ordinary skill in the art would have readily recognized the desirability and advantages of modifying Krishnan by employing virus signatures, such as disclosed by Chi, in order to detect the viruses without having to store the entire virus code.

In considering the virus signature files being stored on non-volatile solid state memory on the network adapter, Krishnan shows storing virus detection applets and program code implementing a virtual machine for execution of programs in ROM and battery backed RAM for long term storage (see column 2, line 65 – column 3, line 12). Therefore it would be obvious to also store the virus signature files with the applets and program code in order for the applets executing the virus scan to use the signatures to detect viruses.

As per claim 3, Krishnan in view of Chi further disclose that the processor is capable of being user-configured locally (see Krishnan column 3, lines 24-26)

As per claim 4, Krishnan in view of Chi further disclose that the processor is capable of being user-configured remotely via a network connection with the network adapter (see Krishnan column 3, lines 36-37).

As per claim 6, Krishnan in view of Chi further disclose that the manner in which the scanning is performed is capable of being user-configured (see Krishnan column 5, lines 16-32).

As per claim 7, Krishnan in view of Chi further disclose that the settings of the network adapter are capable of being user-configured (see Krishnan column 5, lines 33-35).

As per claim 12, Krishnan in view of Chi further disclose that the processor is capable of denying received packets that fail the scan (see Krishnan column 5, lines 16-23).

As per claim 13, Krishnan in view of Chi further disclose that the scan is performed based on user settings (see Krishnan column 3, lines 2-6).

As per claims 14,27,28, Krishnan in view of Chi discloses a method for scanning network traffic on a network adapter, comprising:

receiving packets at a network adapter including a processor positioned thereon, the network adapter being capable of being installed on an end-point computer (see Krishnan column 2, lines 33-39, where network adapter is considered the software-controlled modem);

virus scanning and content scanning of the packets utilizing the processor, the content scanning including scanning for unwanted content other than viruses (see Krishnan column 5, lines 16-28, where processor executes applets to scan incoming data and content is considered "junk e-mail"); and

conditionally taking security measures if the packets fail the scan (see Krishnan column 5, lines 16-23);

wherein the virus scanning utilizes virus signature files to scan for known types of malicious programs or data (see Chi column 3, lines 47-65);

wherein the virus signature files are stored on non-volatile solid state memory on the network adapter (please see discussion above regarding solid state memory, i.e. program files are stored in ROM, therefore it would be obvious to store the signature files there as well);

wherein the processor is capable of being user-configured (see Krishnan column 5, lines 33-35 and lines 55-57, where a user can buy an applet that is used to control modem (i.e. the modem processor));

wherein the processor is capable of determining whether received packets are of interest (see Krishnan column 5, lines 16-23, where packets of interest are considered viruses, etc.), passing received packets that are not of interest to the end-point computer (see Krishnan column 5, lines 16-23, i.e. if not a virus than packets is not discarded), and scanning received packets that are of interest (see Krishnan column 5, lines 16-23, i.e. scanning packets for viruses).

As per claims 16-20,25-26, see rejection for claims 2-8,10-13 above.

As per claim 29, Krishnan in view of Chi disclose a network adapter system, comprising:

a processor positioned on a network adapter coupled between a computer and a network, the processor including a packet assembly module, random access memory (RAM), and a scanner module (see column 2, lines 56-65, where it is implied if not inherent that there is a packet assembly module in order to receive data from the outside see column 5, lines 16-18 for scanner module);

a user interface driver for identifying network traffic of interest transmitted between the computer and the network (see Krishnan column 5, lines 24-31);

wherein the processor is adapted for discerning and virus scanning and content scanning of network traffic of interest transmitted between the computer and the network (see Krishnan column 5, lines 16-31);

wherein the virus scanning utilizes virus signature files to scan for known types of malicious programs or data (see Chi column 3, lines 47-65);

wherein the virus signature files are stored on non-volatile solid state memory on the network adapter (please see discussion above regarding solid state memory, i.e. program files are stored in ROM, therefore it would be obvious to store the signature files there as well);

wherein the network adapter receives the network traffic (see Krishnan column 5, lines 16-23);

wherein the processor is capable of being user-configured (see Krishnan column 5, lines 33-35 and lines 55-57, where a user can buy an applet that is used to control modem (i.e. the modem processor));

wherein the processor is capable of determining whether received packets are of interest (see Krishnan column 5, lines 16-23, where packets of interest are considered viruses, etc.), passing received packets that are not of interest to the end-point computer (see Krishnan column 5, lines 16-23, i.e. if not a virus than packets is not discarded), and scanning received packets that are of interest (see Krishnan column 5, lines 16-23, i.e. scanning packets for viruses).

As per claim 30, Krishnan in view of Chi further disclose that the content scanning enforces operational policies of an organization (see Krishnan column 5, lines 24-30).

As per claims 31,40, Krishnan in view of Chi further disclose that the policies include detecting entities selected from the group consisting of harassing content, pornographic content, junk e-mails, and misinformation (see Krishnan column 5, lines 24-30).

As per claim 34, Krishnan in view of Chi further disclose that the packets that are of interest include executable files (see Krishnan column 5, lines 16-23).

As per claim 38, Krishnan in view of Chi further disclose that the network adapter includes a cable modem adapter (see column 6, lines 36-45).

As per claim 39, Krishnan in view of Chi further disclose that the network adapter includes a broadband adapter (i.e. cable modem).

4. Claims 9,22,43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Krishnan in view of Chi as applied to claims 1,14 above, and further in view of Makinson et al. (US 7,023,861), herein referred to as Makinson.

As per claims 9,22, although the system disclosed by Krishnan in view of Chi shows substantial features of the claimed invention (discussed above), it fails to disclose that the packets of interest are based on an associated protocol.

Nonetheless, these features are well known in the art and would have been an obvious modification of the system disclosed by Krishnan in view of Chi, as evidenced by Makinson.

In an analogous art, Makinson discloses a bridge with a built in scanner connected to an end-user computer (see Fig. 5), where the scanning of packets may be selected based on the certain types of protocols (see column 4, lines 50-57).

Given the teaching of Makinson, a person having ordinary skill in the art would have readily recognized the desirability and advantages of modifying Krishnan in view of Chi by employing protocol specific scanning, such as disclosed by Makinson, in order to relieve the processor from scanning unnecessary packets.

As per claim 43, Makinson further discloses that the received packets that are not of interest to the end-point computer bypass the scanning (see column 4, lines 50-57).

5. Claims 5,18,33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Krishnan in view of Chi as applied to claims 1,14 above, and further in view of Bonomo et al. (US 6,658,562), herein referred to as Bonomo.

Although the system disclosed by Krishnan in view of Chi shows substantial features of the claimed invention (discussed above), it fails to disclose that memory is user protected by configuring a network adapter BIOS with a password that only a user can change.

Nonetheless, these features are well known in the art and would have been an obvious modification of the system disclosed by Krishnan in view of Chi, as evidenced by Bonomo.

In an analogous art, Bonomo discloses a system for setting different BIOS configurations stored in a memory device (see Abstract). Further showing setting a password to view information in a BIOS setup program or to change configuration (see column 4, lines 11-21 and 30-41).

Given the teaching of Bonomo, a person having ordinary skill in the art would have readily recognized the desirability and advantages of modifying Krishnan in view of Chi by employing a password protected BIOS, such as disclosed by Bonomo, in order to prevent unwanted users from changing settings without authorization.

6. Claims 35-36, are rejected under 35 U.S.C. 103(a) as being unpatentable over Krishnan in view of Chi.

As per claim 35,36, Krishnan in view of Chi does not expressly disclose that the network adapter includes a Peripheral Component Interconnect (PCI) card and/or an Industry Standard Architecture (ISA) card. However, Krishnan does disclose that the adapter can be an add-in card for installation in an expansion slot of a computer comprising an expansion bus interface (see column 2, lines 47-50). At the time of the invention, a person having ordinary skill in the art would have recognized that PCI and ISA are commonly used and well known expansion bus interfaces. Therefore it would have been obvious to make network adapters for both PCI and ISA in order to provide an adapter compatible with most computers.

7. Claims 35-37 is rejected under 35 U.S.C. 103(a) as being unpatentable over Krishnan in view of Chi as applied to claim 1 above, and further in view of Sridhar et al. (US 5,799,064), herein referred to as Sridhar.

As per claims 35,36 although the system disclosed by Krishnan shows substantial features of the claimed invention (discussed above), it fails to disclose that the network adapter includes a Peripheral Component Interconnect (PCI) card and/or an Industry Standard Architecture (ISA) card.

Nonetheless, these features are well known in the art and would have been an obvious modification of the system disclosed by Krishnan in view of Chi, as evidenced by Sridhar.

In an analogous art, Sridhar discloses an apparatus interfacing between a communication channel and a processor for data transmission and reception (see Abstract) further showing that the apparatus may be connected to a bus such as an ISA or PCI bus (see column 3, line 63 – column 4, line 2).

Given the teaching of Sridhar, a person having ordinary skill in the art would have readily recognized the desirability and advantages of modifying Krishnan by employing a network adapter including a PCI and/or ISA card, such as disclosed by Chi, in order to connect to the bus of the end-point computer.

As per claim 37, Krishnan in view of Chi in view of Sridhar further disclose that the network adapter includes an Integrated Services Digital Network (ISDN) adapter (see Sridhar column 4, lines 11-19).

8. Claim 41 is rejected under 35 U.S.C. 103(a) as being unpatentable over Krishnan in view of Chi as applied to claim 1 above, and further in view of Horvitz et al. (US 6,161,130), herein referred to as Horvitz..

Although the system disclosed by Krishnan shows unwanted content includes junk e-mails and misinformation (see column 5, lines 24-25 for junk e-mail and column 5, lines 16-18, where Trojan horses are considered misinformation), it fails to disclose harassing content and pornographic content.

Nonetheless, these features are well known in the art and would have been an obvious modification of the system disclosed by Krishnan in view of Chi, as evidenced by Horvitz.

In an analogous art, Horvitz discloses a system that detects electronic mail messages that the recipient is likely to consider junk (see Abstract). Further disclosing that the unwanted messages include harassing content and pornographic content (see column 9, lines 44-51, where harassing content is considered abusive or insulting messages).

Given the teaching of Horvitz, a person having ordinary skill in the art would have readily recognized the desirability and advantages of modifying Krishnan in view of Chi by employing a harassing

content and pornographic content filter, such as disclosed by Horvitz, in order to keep the incoming data safe for users.

9. Claim 42 is rejected under 35 U.S.C. 103(a) as being unpatentable over Krishnan in view of Chi in view of Makinson as applied to claim 9 above, and further in view of Lerche et al. (US 5,511,163), herein referred to as Lerche.

As per claim 42, although the system disclosed by Krishnan in view of Chi in view of Makinson shows substantial features of the claimed invention (discussed above), it fails to disclose that a predetermined amount of the received packets are assembled for determining whether the received packets are of interest.

Nonetheless, these features are well known in the art and would have been an obvious modification of the system disclosed by Krishnan in view of Chi in view of Makinson, as evidenced by Lerche.

In an analogous art, Lerche discloses a system with a computer and a network adapter that is able to receive all information on the network and the adapter can perform an assembling and scanning of all files on the network and carry out a recognition of virus signatures (see Abstract). Lerche also discloses that a predetermined amount of the received packets are assembled for determining whether the received packets are of interest (see column 1, lines 38-49, *showing that a predetermined amount of packets (i.e. all packets) are assembled into one file and then determined if they are of interest by scanning them for detection of virae*).

Given the teaching of Lerche, a person having ordinary skill in the art would have readily recognized the desirability and advantages of modifying Krishnan in view of Chi in view of Makinson by employing assembling of the received packets, such as disclosed by Lerche, in order to catch all potential viruses on a network of computers.

Response to Arguments

10. Applicant's arguments filed January 16, 2008 have been fully considered but they are not persuasive.

(A) Applicant contends that Krishnan fails to teach a processor including a packet assembly module.

In considering (A), the Examiner respectfully disagrees. Applicant asserted that the applicants claimed "packet assembly module" is to be read in view of its plain and ordinary meaning. However, it is not clearly claimed what the "packet assembly module" does when assembling packets. One of ordinary skill in the art could interpret the packet assembly module as part of the modem taking analog data from the telephone lines and assembling a packet so that the computer attached to the modem can understand the data. A second interpretation by one of ordinary skill in the art for the "packet assembly module" can be seen as assembling the packets so that a scanner can determine if there is a program hidden among the packets that are potentially dangerous. In either case, the Examiner believes that Krishnan shows evidence of both. In considering the first scenario of the "packet assembly module" assembling packets from analog data, Krishnan discloses that the modem is coupled to a telephone line and to a computer (sees column 2, lines 35-39, the telephone line implying an analog signal). In order for the computer to understand, the analog data has to be converted to a packet (i.e. formatted digital data) by the modem. Therefore, it is a necessary step to assemble a packet for the computer to understand data received by the modem. In considering the second scenario, Krishnan also provides evidence that a packet is assembled for scanning by an applet. Krishnan shows that applets may be used to scan incoming data for potentially hazardous programs (see column 5, lines 16-30). It is necessary that the packets containing these programs have to be assembled in order to be scanned. Otherwise the scanner will not know which packet belongs to which program. A program has to eventually be assembled from the many different packets that the modem receives in order to determine if the program is hazardous.

B) Applicant contends that Krishnan fails to disclose that the processor is capable of determining whether received packets are of interest, wherein the processor is capable of passing

received packets that are not of interest to the end-point computer, and wherein the processor is capable of scanning received packets that are of interest.

In considering B), the Examiner respectfully disagrees. Krishnan teaches that the packets are scanned for potentially hazardous programs. The Examiner believes that the "packets of interest" are considered packets that contain the potentially hazardous programs. While the processor performs the scanning, the packets of interests are determined and either discarded or triggers an alert for the user that a potential rogue program is found (see column 5, lines 16-23). In Krishnan's system, it appears that all packets are scanned (i.e. the ones of interest and the ones not of interest). However, it is not claimed that when determining, the ones not of interest are not scanned. Therefore, Krishnan's system shows that the processor is capable of scanning received packets that are of interest and either discarding them or alerting the user to a potential rogue program. In considering the packets that are not of interest being sent to the end-point computer, it is inherent that the packets are sent to the end-point computer because the job of the modem is to receive packets and send them to the end-point computer and they are not of interest so they will not be discarded or alert the user of a potential rogue program. See column 1, lines 35-44, describing the modems job for receiving data from the Internet and passing the data to a computer to render a web page.

C) Applicant contends that Krishnan fails to disclose that the processor is capable of being user-configured.

In considering C), the Examiner respectfully disagrees. It is clear that Krishnan shows a user can purchase an applet to control the modem (see column 5, lines 33-35 and lines 55-57, where a user can buy an applet that is used to control modem (i.e. the modem processor)); It is unclear if the claim limitation means a user can configure the processor by removing/installing jumpers, or soldering new wires to cause the processor to perform something different, or installing programs to cause the processor to perform a new function, etc. The Examiner believes that Krishnan shows a user can configure the processor by installing new applets that cause the processor to perform a new task (e.g. a new virus scanning program).

D) Applicant contends that Krishnan fails to disclose enforcing operational policies of an organization.

In considering D), the Examiner respectfully disagrees. It is noted that in the specification, operational policies of an organization can be detecting harassing or pornographic content, junk e-mails, viruses, etc. (see Specification page 9, lines 7-10). Krishnan shows an applet providing filtering of junk e-mail and other unwanted data (see column 5, lines 25-30) and scanning for viruses (see column 5, lines 16-20). It is believed that this teaching is enough evidence to support the enforcement of operational policies.

Conclusion

11. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to PHILIP J. CHEA whose telephone number is (571)272-3951. The examiner can normally be reached on M-F 6:30-4:00 (1st Friday Off).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Glenn Burgess can be reached on 571-272-3949. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Glenton Burgess/
Supervisory Patent Examiner, Art Unit 2153

Philip J Chea
Examiner
Art Unit 2153

PJC 3/11/08